CERT

Evaluating and Improving Cybersecurity Capabilities of the Electricity Critical Infrastructure

May 2015

Katie Stewart

Cyber Risk and Resilience Management Team
CERT Division
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

Software Engineering Institute | **Carnegie Mellon University**

Notices

Outline

Electric Grid: Yesterday vs. Today

Development Approach

A Family of Cybersecurity Maturity Models

Model Architecture

- Domains
- Scaling
- Diagnostic Methodology

Using the Model

Relationship to NIST Cybersecurity Framework

CMU – SEI – CERT® Division

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University

- Basic and applied research in partnership with government and private organizations

- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT® Division – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at SEI

- Focused on internet security, digital investigation, secure systems, insider threat, operational resilience, vulnerability analysis, network situational awareness, and coordinated response

Cyber Risk and Resilience Management Team

Engaged in

- Applied research
- Education & training
- Putting into practice
- Enabling our federal, state, and commercial partners

In areas dealing with

- Maturity models
- Operational resilience
- Resilience management
- Operation risk management
- Cybersecurity maturity models
- Integration of cybersecurity, business continuity, & disaster recovery

TODAY: Smart Grid
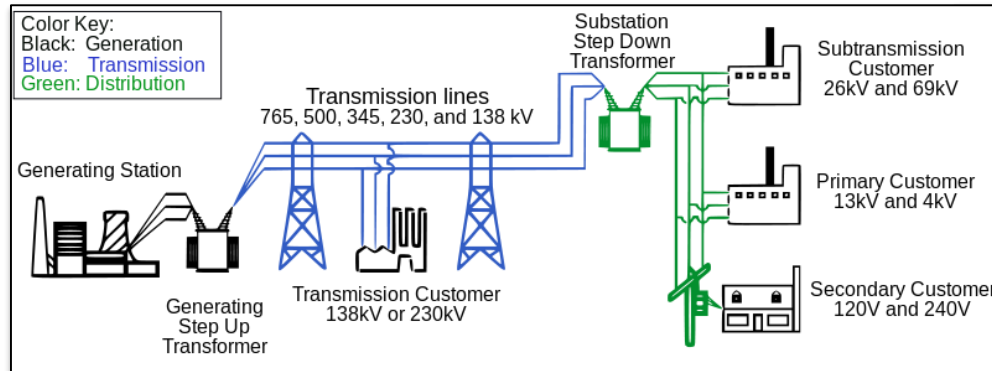
Legacy Electrical Grid
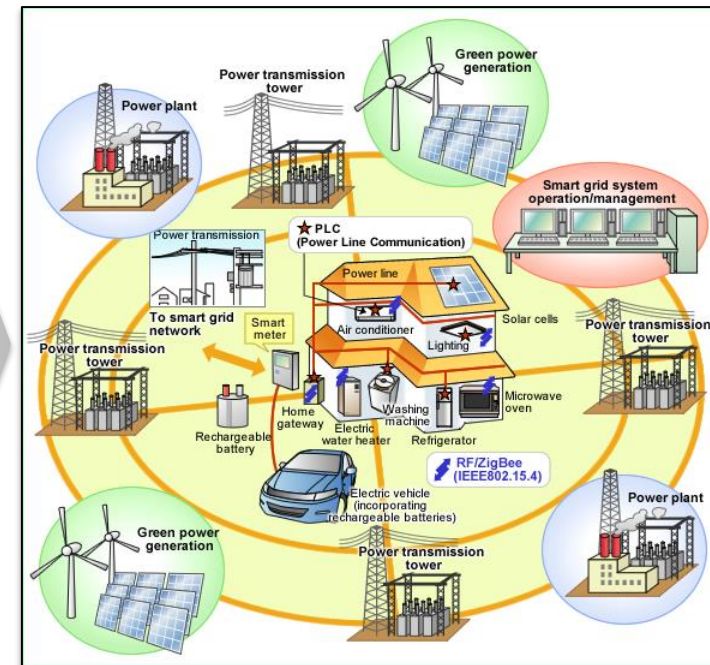
Modern Smart Grid

INCREASED FUNCTIONALITY & EFFICIENCY

INCREASED OPERATIONAL RISK

Strong Sponsorship & Collaboration

White House initiative

Led by Department of Energy

In partnership with DHS

In collaboration with energy sector asset owners and operators

SEI model architect

Development Approach

Public-Private Partnership

Best Practices and existing cybersecurity resources

Review of cyber threats to the subsectors

Descriptive, Not Prescriptive

Fast-Paced Development

Pilot to Test, Validate, and Improve

The Approach: Maturity Model

An organized way to convey a path of experience, wisdom, perfection, or acculturation.

A Maturity Progression for Authentication
Three-factor authentication
Two-factor authentication
Addition of changing every 60 days
Use of strong passwords
Use of simple passwords`
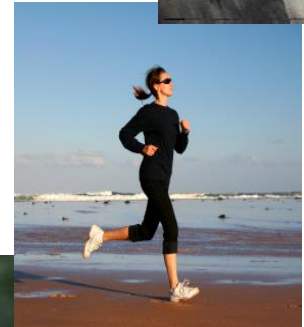
A Family of Cybersecurity Maturity Models
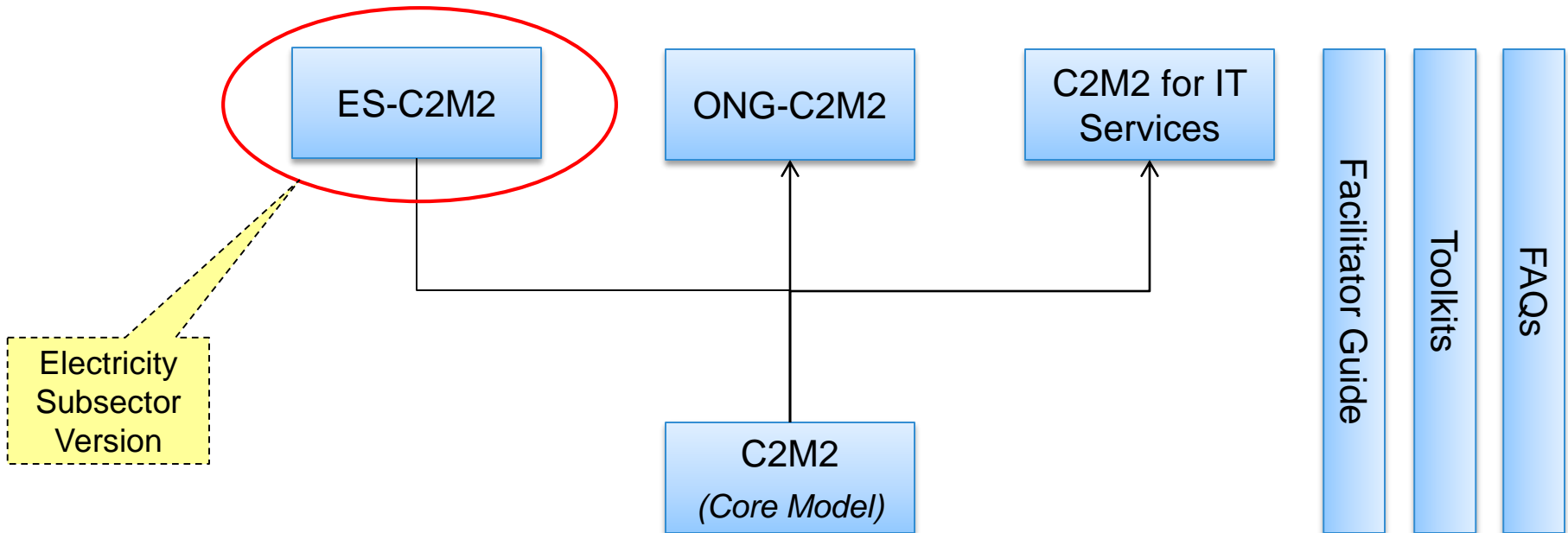
Enabling Consistent Applicability to Complex Organizations

Electricity Subsector

Electricity portion of the energy sector

Includes

- Generation
- Transmission
- Distribution
- Marketing

Model Architecture

A Maturity Model	Domains (a.k.a. Process Areas)
	Scaling
	Diagnostic Methodology
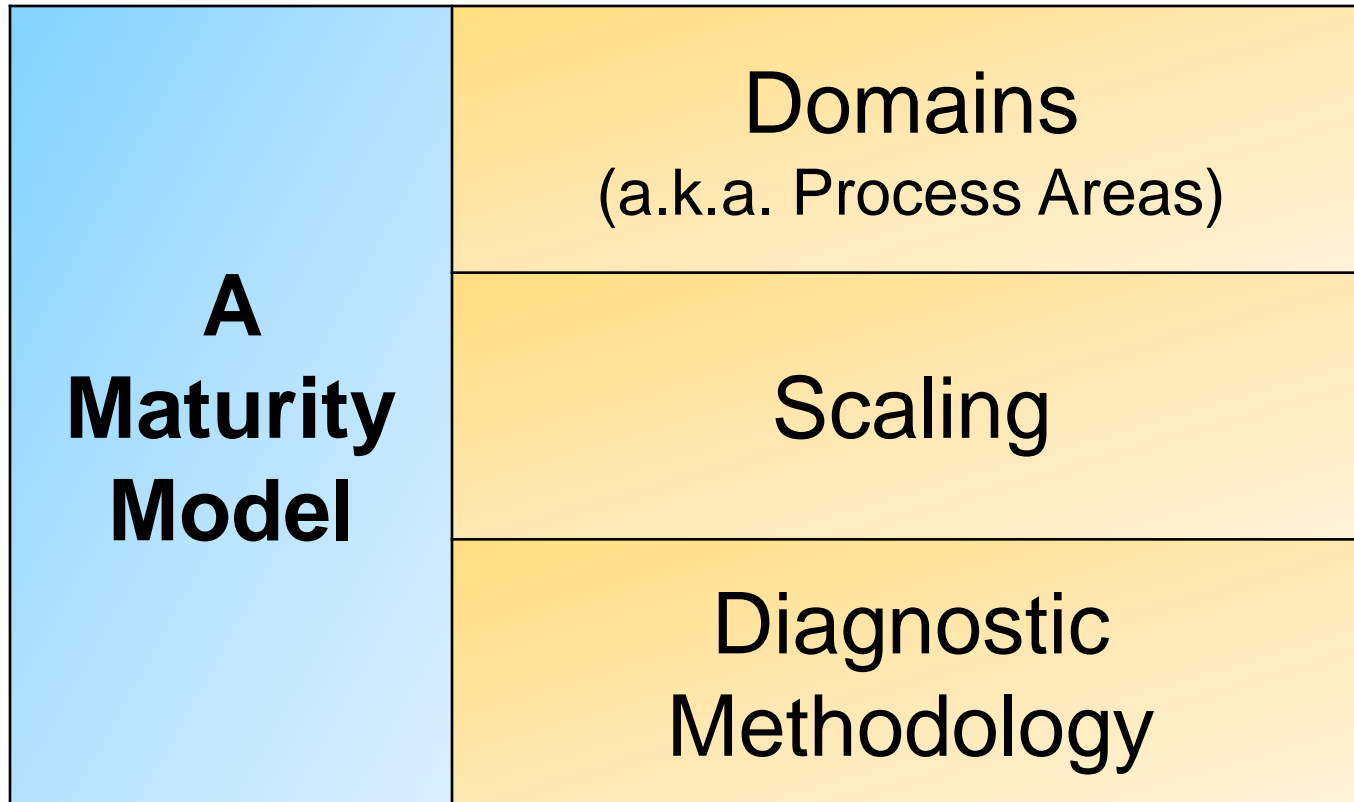
Domains that C2M2 Examines

RM Risk Management	**ACM** Asset, Change, and Configuration Management	**IAM** Identity and Access Management	**TVM** Threat and Vulnerability Management
SA Situational Awareness	**ISC** Information Sharing and Communications	**IR** Event and Incident Response, Continuity of Operations	**EDM** Supply Chain and External Dependencies Management
	WM Workforce Management	**CPM** Cybersecurity Program Management	

Domains are logical groupings of cybersecurity practices

CERT | Software Engineering Institute | Carnegie Mellon University

Model Architecture

A Maturity Model	Domains (a.k.a. Process Areas) ✓	
	Scaling	
	Diagnostic Methodology	

C2M2 Structure

4 Maturity Indicator Levels: Defined progressions of practices

Maturity Indicator Levels

3 Managed

2 Performed

1 Initiated

0 Not Performed

RISK | ASSET | ACCESS | THREAT | SITUATION | SHARING | RESPONSE | DEPENDENCIES | WORKFORCE | CYBER

10 **Model Domains**: Logical groupings of cybersecurity practices

C2M2 Structure

Maturity Indicator Levels

3 Managed

2 Performed

1 Initiated

0 Not Performed

4 Maturity Indicator Levels: Defined progressions of practices

Each cell contains the defining practices for the domain at that maturity indicator level

RM ACM IAM TVM SA ISC IR EDM WM CPM

10 **Model Domains**: Logical groupings of cybersecurity practices

C2M2 Maturity Indicator Levels

Level	Name	Description
MIL0	Not Performed	• MIL1 has not been achieved in the domain
MIL1	Initiated	• Initial practices are performed, but may be ad hoc
MIL2	Performed	• Practices are documented • Stakeholders are involved • Adequate resources are provided for the practices • Standards or guidelines are used to guide practice implementation • Practices are more complete or advanced than at MIL1
MIL3	Managed	• Domain activities are guided by policy (or other directives) • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are clearly assigned to personnel with adequate skills and knowledge • Practices are more complete or advanced than at MIL2

Domain Structure

Model		
	Domain	Model contains 10 domains
	Purpose Statement	Summarizes the overall intent of the domain
	Introductory Notes	Provide an overview of the domain objectives
	Approach Objectives	One or more per domain; unique to each domain
	Specific Practices at MIL1	
	Specific Practices at MIL2	Each specific objective is supported by a progression of practices that are unique to the domain and are ordered by maturity indicator level (MIL)
	Specific Practices at MIL3	
	Management Objective	One per domain; similar across domains
	Common Practices at MIL2	
	Common Practices at MIL3	The Management Objective is supported by a progression of practices at MIL2 and MIL3 that are similar in each domain."

Model Architecture

A Maturity Model	Domains (a.k.a. Process Areas) ✓
	Scaling ✓
	Diagnostic Methodology

C2M2 Self-Evaluation

The C2M2 models are supported by a survey-based self-evaluation

An organization can use the survey (and associated scoring tool) to evaluate its implementation of the model practices
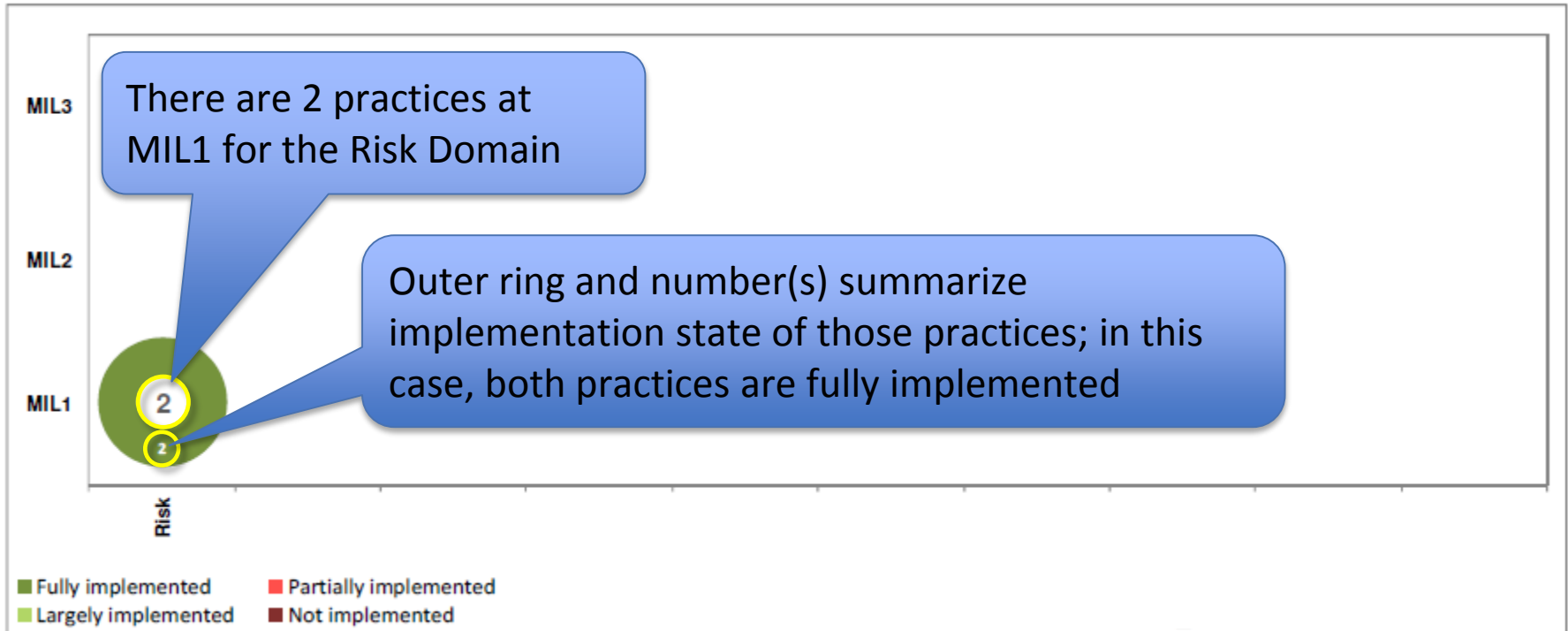

To complete the survey, an organization selects its level of implementation for the model practice from a 4-point answer scale

4-Point Answer Scale

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	Complete, but with a recognized opportunity for improvement
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

C2M2 Sample Summary Score
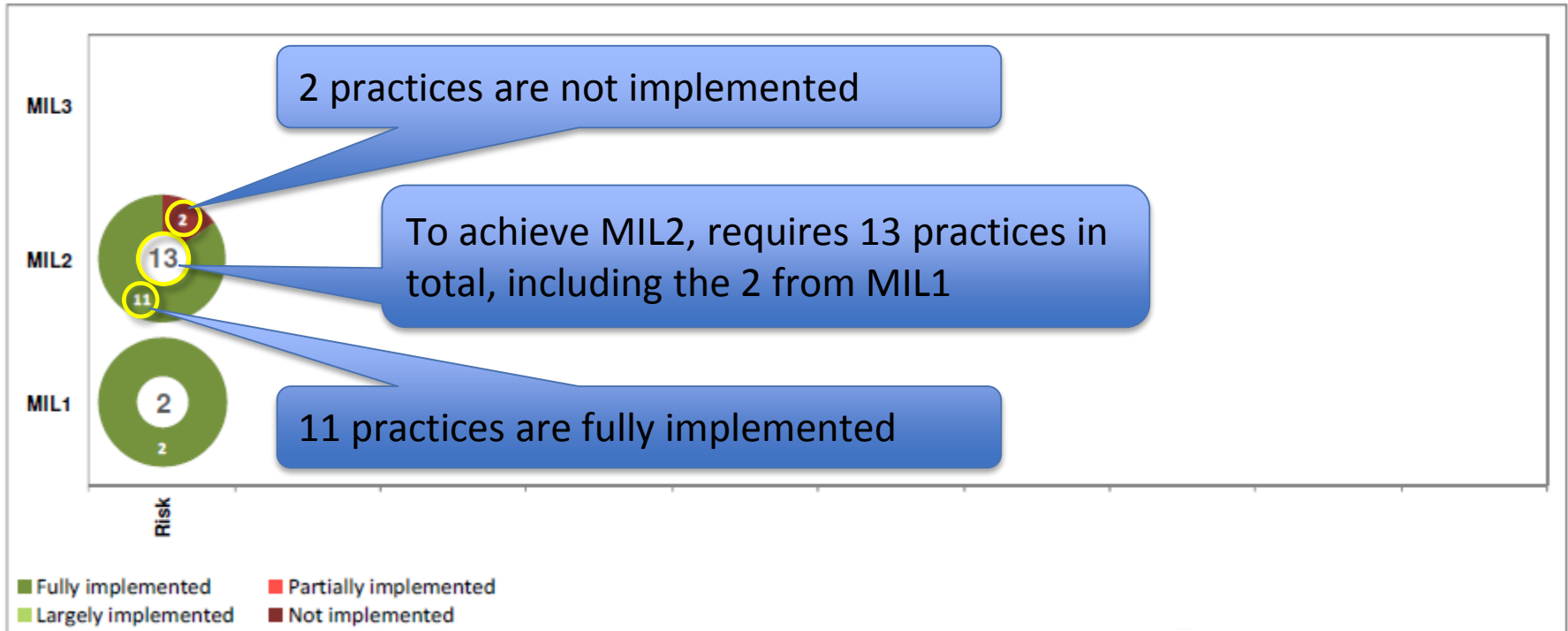
C2M2 Sample Summary Score

C2M2 Sample Summary Score

C2M2 Sample Summary Score

Legend:
- Fully implemented
- Partially implemented
- Largely implemented
- Not implemented

	Risk	Asset	Access	Threat	Situation	Sharing	Response	Dependencies	Workforce	Cyber
MIL Rating	1	0	2	3	3	3	3	1	2	0

Software Engineering Institute | Carnegie Mellon University
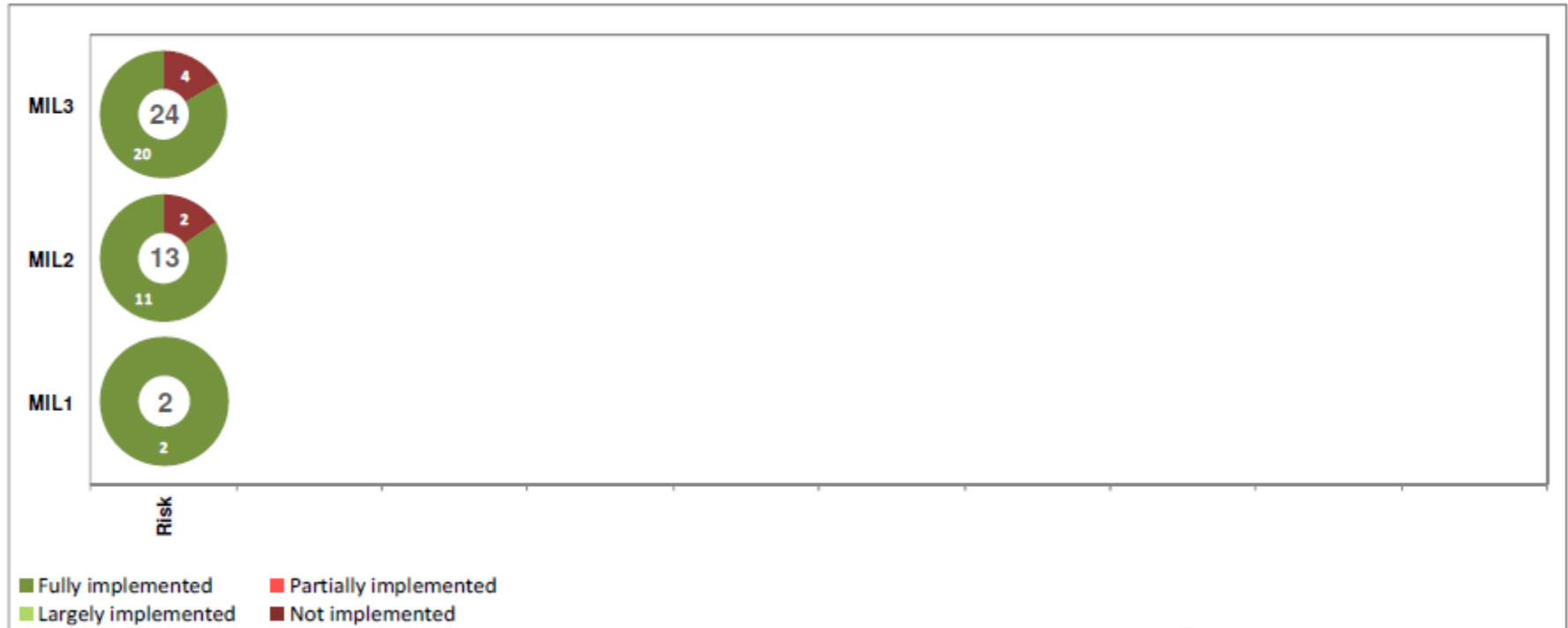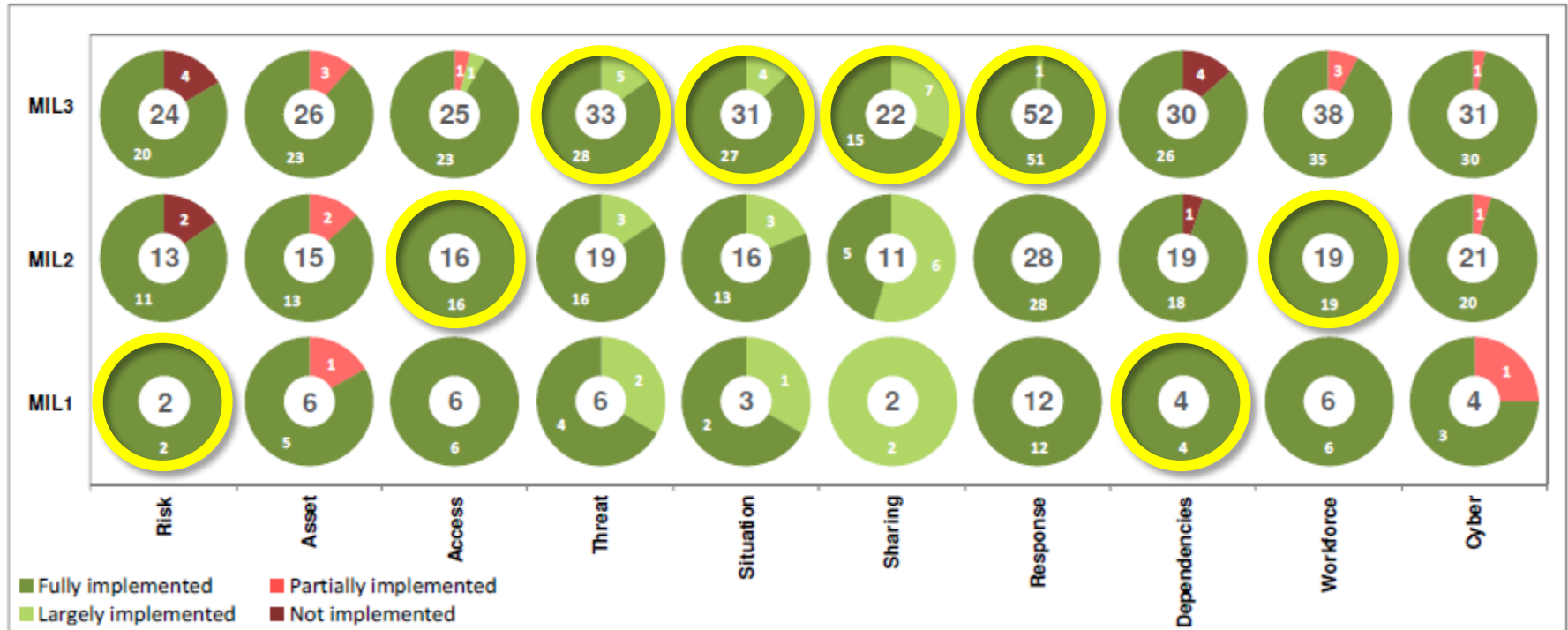
C2M2 Sample Summary Score

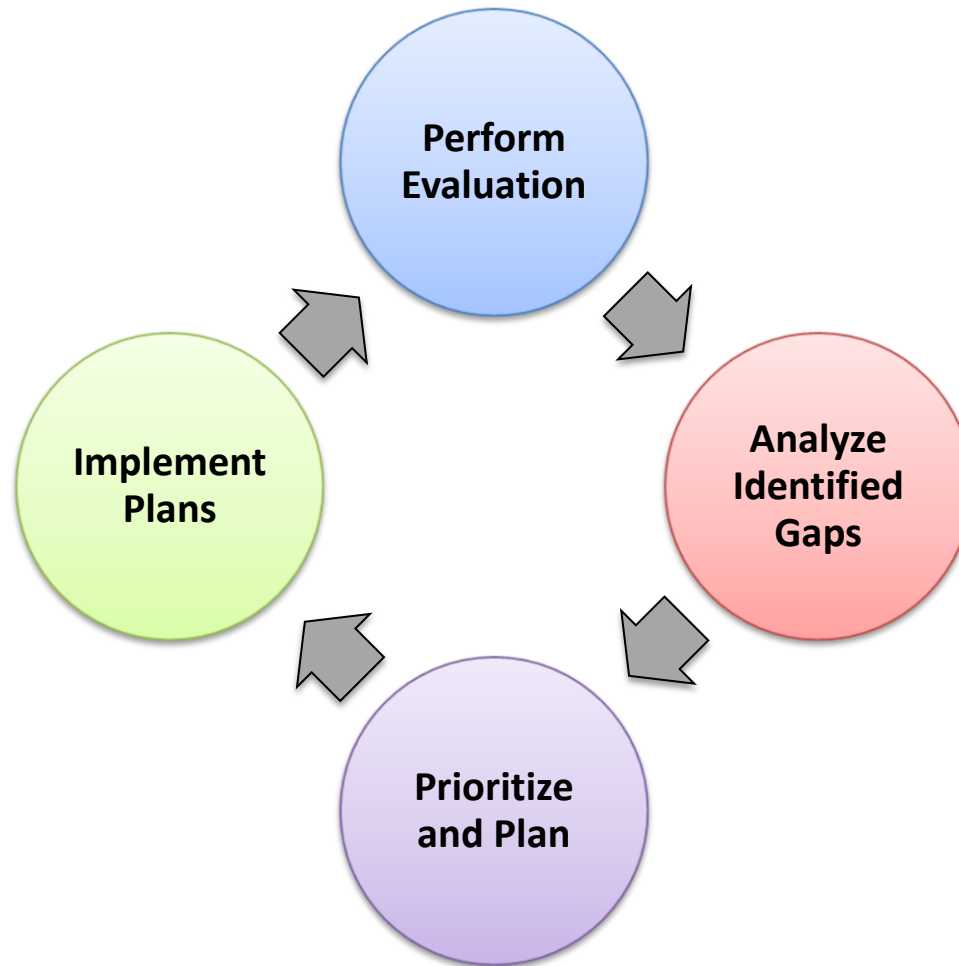| 1. Establish Cybersecurity Risk Management Strategy			
MIL1		*No practice at MIL1*	
MIL2	a.	There is a documented cybersecurity risk management strategy	FI
	b.	The strategy provides an approach for risk prioritization, including consideration of impact	LI
MIL3	c.	Organizational risk criteria (tolerance for risk, risk response approaches) are defined	NI
	d.	The risk management strategy is periodically updated to reflect the current threat environment	PI
	e.	An organization-specific risk taxonomy is documented and is used in risk management activities	NI
2. Manage Cybersecurity Risk			
MIL1	a.	Cybersecurity risks are identified, at least in an ad hoc manner	PI
	b.	Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner	LI
MIL2	c.	Risk assessments are performed to identify risks in accordance with the risk management strategy	LI
	d.	Identified risks are documented	LI
	e.	Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy	LI
	f.	Identified risks are monitored in accordance with the risk management strategy	PI
	g.	Risk analysis is supported by network (IT and/or OT) architecture	PI
MIL3	h.	The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	PI
	i.	A current cybersecurity architecture is used to support risk analysis	NI
	j.	A risk register (a structured repository of identified risks) is used to support risk management activities	NI

C2M2 Sample Summary Score

MIL 1		MIL 2												MIL 3									
2a	2b	1a	1b	2c	2d	2e	2f	2g	3a	3b	3c	3d		1c	1d	1e	2h	2i	2j	3e	3f	3g	3h	3i

Risk Management

- ■ Fully implemented
- ■ Largely implemented
- ■ Partially implemented
- ■ Not implemented

Establish Cybersecurity Risk Management Strategy — 5 (1 fully, 1 largely, 1 partially, 2 not)

Manage Cybersecurity Risk — 10 (4 largely, 4 partially, 2 not)

Management Activities — 9 (1 fully, 3 largely, 3 partially, 2 not)

CERT | Software Engineering Institute | Carnegie Mellon University

Model Architecture

A Maturity Model	Domains (a.k.a. Process Areas) ✓
	Scaling ✓
	Diagnostic Methodology ✓

Using the C2M2 Models

Recommended Process for Using Results

	Inputs	Activities	Outputs
Perform Evaluation	1. C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct C2M2 Self-Evaluation Workshop with appropriate attendees	C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	Prioritized implementation plan	1. Track progress to plan 2. Re-evaluate periodically or in response to major change	Project tracking data

Relationship to NIST Cybersecurity Framework

The U.S. Department of Energy (DOE) has developed guidance on using the NIST Cybersecurity Framework for the Energy Sector

DOE guidance highlights C2M2 models as an approach to using the NIST Cybersecurity Framework

ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE

JANUARY 2015

U.S. DEPARTMENT OF ENERGY
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY

◉ ENERGY.GOV
Office of Electricity Delivery & Energy Reliability

Search Energy.gov | 🔍

SERVICES | INFORMATION CENTER | MISSION | ABOUT US | OFFICES >

Home » Services » Cybersecurity » Cybersecurity Capability Maturity Model (C2M2) Program
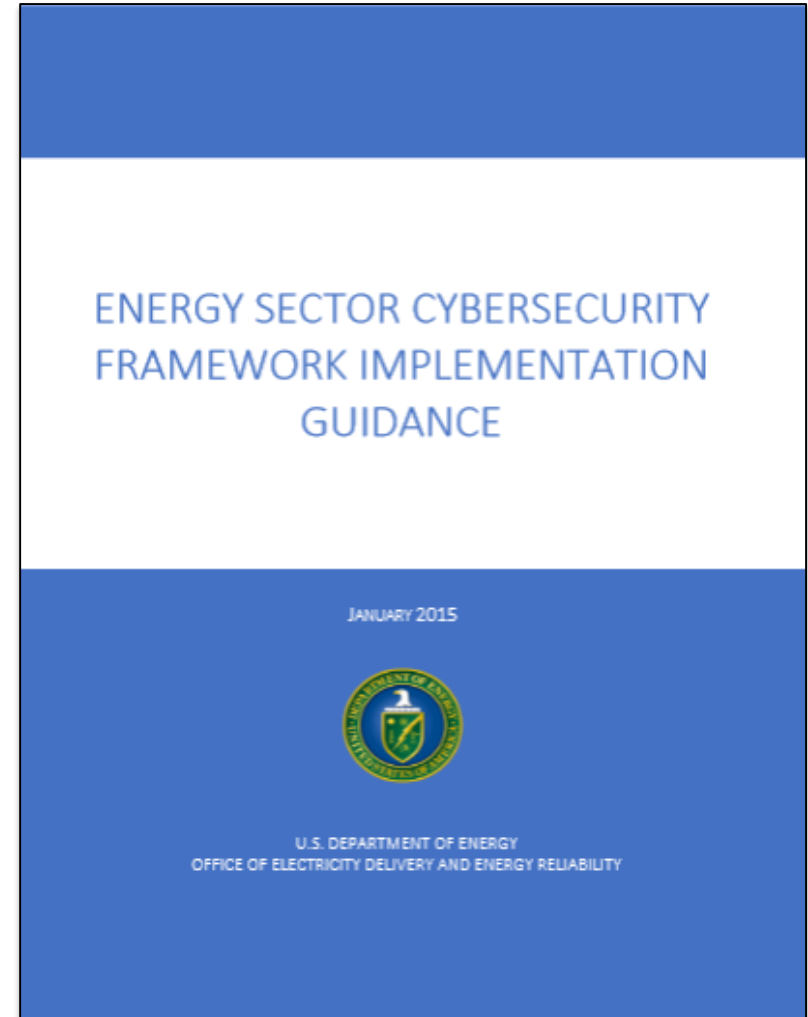
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) PROGRAM

Electricity Advisory Committee

Technology Development

Electricity Policy Coordination and Implementation

DOE Grid Tech Team

Energy Assurance

Cybersecurity

NIST Framework

C2M2 Program

Cybersecurity Capability Maturity Model

ES-C2M2

ONG-C2M2

Cybersecurity Risk Management Process

Energy Delivery Systems Cybersecurity

RELATED LINKS

Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity"

NIST Framework

Use of the NIST Cybersecurity Framework & DOE C2M2

Cybersecurity Capability Maturity Model (C2M2) Program

C2M2 Model

Electricity Subsector C2M2 Model

Podcast - Electricity Subsector C2M2 Model

Oil and Natural Gas Subsector C2M2 Model

The Cybersecurity Capability Maturity Model (C2M2) program is a public-private partnership effort that was established as a result of the Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. The C2M2 helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity

For More Information

DOE Cybersecurity Capability Maturity Model Program

- http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

ONG-C2M2

- http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity

ES-C2M2

- http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

Core C2M2

- http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity-capability-maturity-model-c2m2

SEI Resilience Management Program

- http://www.cert.org/resilience/

Thank you for your attention…

Additional Material

Model Domains (1-2 of 10)

Domain	Description
Asset, Change, and Configuration Management (ACM)	Manage the organization's operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives, including activities to: • Identify, inventory, and prioritize assets, • Manage asset configurations, and • Manage changes to assets and to the asset inventory.
Workforce Management (WM)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives. • Responsibilities • Workforce controls • Knowledge, skills, and abilities • Awareness

Model Domains (3-4 of 10)

Domain	Description

Identity and Access Management (IAM)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.
	
	    • Identity management
	    • Access management

Risk Management (RM)	Establish, operate, and maintain a cybersecurity risk management and mitigation program to identify and manage cybersecurity risk to the organization and its related interconnected infrastructure and stakeholders.
	
	    • Strategy
	    • Sponsorship
	    • Program

Model Domains (5-6 of 10)

Domain	Description
Supply Chain and External Dependencies Management (EDM)	Establish and maintain controls to manage the cybersecurity risk associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives. • Dependency identification • Risk management • Cybersecurity requirements
Threat and Vulnerability Management (TVM)	Establish and maintain plans, procedures, and technologies to identify, analyze, and manage cybersecurity threats and vulnerabilities, commensurate with the risk to critical infrastructure and organizational objectives. • Threat management • Vulnerability management • Cybersecurity patch management • Assessments

Model Domains (7-8 of 10)

Domain	Description
Event and Incident Response, Continuity of Operations (IR)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity incidents and to sustain critical functions throughout a cyber event, commensurate with the risk to critical infrastructure and organizational objectives. • Detect events • Declare incidents • Respond to incidents • Manage continuity
Situational Awareness (SA)	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives. • Logging • Monitoring • Awareness

Model Domains (9-10 of 10)

Domain	Description
Information Sharing and Communications (ISC)	Establish and maintain relationships with internal and external entities to share information, including threats and vulnerabilities, in order to reduce risks and increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives. • Communication • Analysis • Coordination
Cybersecurity Program Management (CPM)	Establish and maintain a cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure. • Strategy • Sponsorship • Program • Architecture

C2M2 Maturity Indicator Levels Example

Specific Characteristics for the ASSET domain	
MIL0	

MIL1	1. Asset inventory
	
	    a. There is an inventory of OT (operational technology) and IT (information technology) assets that are important to the delivery of the function
	
	    …

MIL2	…

MIL3	1. Asset inventory
	
	    a. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis
	
	    b. Asset prioritization is informed by risk analysis
	
	    …

Progress from one MIL to the next involves more complete or more advanced implementations of the core activities in the domain.

The organization is also expected to be performing additional activities at higher levels consistent with their risk strategy.

A Dual-Progression Model

The C2M2 is a dual progression model

Two things are progressing across the maturity indicator levels:

1. **Approach** – the completeness, thoroughness, or level of development/sophistication of the activity

2. **Management** – the extent to which the practices are ingrained/institutionalized in the organization's operations

Example of Dual Progression

	Manage Cybersecurity Risk	Management Practices
MIL1	a. Cybersecurity risks are identified b. Identified risks are mitigated, accepted, tolerated, or transferred	1. Initial practices are performed but may be ad hoc
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy d. Identified risks are documented e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy f. Identified risks are monitored in accordance with the risk management strategy g. A network (IT and/or OT) architecture is used to support risk analysis	1. Practices are documented 2. Stakeholders of the practice are identified and involved 3. Adequate resources are provided to support the process (people, funding, and tools) 4. Standards and/or guidelines have been identified to guide the implementation of the practices
MIL3	a. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy b. A current cybersecurity architecture is used to support risk analysis c. A risk register (a structured repository of identified risks) is used to support risk management	1. Activities are guided by policies (or other organizational directives) and governance 2. Activities are periodically reviewed to ensure they conform to policy 3. Responsibility and authority for performing the practice is clearly assigned to personnel 4. Personnel performing the practice have adequate skills and knowledge

4-Point Answer Scale – Fully Implemented

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	...vement
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

The practice is performed as described in the model

4-Point Answer Scale – Largely Implemented

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	Complete, but with a recognized opportunity for improvement
Partially implemented	Inco
Not implemented	Abse

The practice is performed substantially as described in the model, but there is some recognized opportunity for improvement that is not material with respect to achieving model, organizational, or critical infrastructure objectives

4-Point Answer Scale – Partially Implemented

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Cor...
Largely implemented	Cor...
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

The practice is performed substantially as described in the model, but there is some recognized opportunity for improvement that is not material with respect to achieving model, organizational, or critical infrastructure objectives

4-Point Answer Scale – Not Implemented

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	...ment
Partially implemented	Inc... there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

The practice is not performed in the organization

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) released its *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) in February 2014

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014
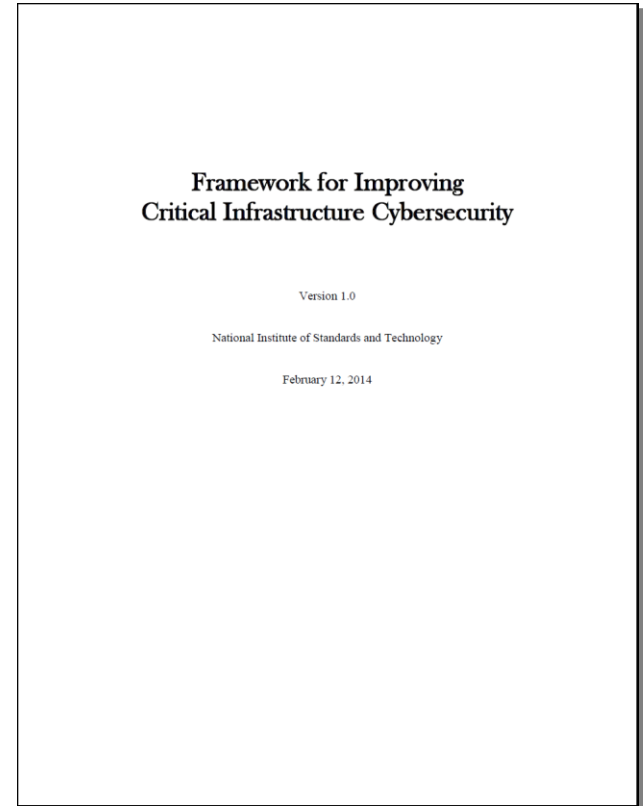
Elements of the Framework

The three main elements of the Framework are the **Core**, the **Implementation Tiers**, and the **Profile**.

The *Core* is a set of "cybersecurity activities, desired outcomes, and applicable informative references that are common across critical infrastructure sectors" within five "functions:" Identify, Protect, Detect, Respond, and Recover.

Tiers describe an organization's approach to "cybersecurity risk and the processes in place to manage that risk," ranging from Tier 1 (Partial) to Tier 4 (Adaptive).

Profiles align the Framework core elements with business requirements, risk tolerance, and organizational resources.